J. Math. Kyoto Univ.
7-2 (1967) 151-160

On the unique factorization theorem for formal power series

By

Hajime NISHIMURA

(Received Aug. 25, 1967)

Let $R\{x_1, \cdots, x_n\}$ be the formal power series ring in a finite number of independent variables $x_1, \cdots, x_n$ with coefficient ring R. It is known that even if R is a unique factorization domain $R\{x_1\}$ is not always so.[1]

We shall denote the following condition for a ring[2] R by $(*)$:

$(*)$ $R\{x_1, \cdots, x_n\}$ *is a unique factorization domain, for any* n *(finite).*

It is noted that $(*)$ is satisfied by a regular semi-local integral domain R, which follows from the fact that a regular local ring is a unique factorization domain. This naturally raises the question whether the unique factorization theorem still holds for the case of infinitely many variables, provided coefficient domain R satisfies $(*)$. The question is only partially answered below (Theorem 1), where notion of formal power series is taken in a wider sense than the usual one.

As for the usual formal power series, what we show is that if R is a Krull ring then $R\{x_1, x_2, \cdots, x_n, \cdots\}$ is also a Krull ring, which is an application of Theorem 1.

The auther wishes to express his sincere thanks to Prof. M. Nagata for his valuable suggestion and encouragement.

1. Let R be a ring, X be a set of indeterminates, card. $X=\aleph^*$. As usual, by a *X-monomial* $(x)^e$ *of degree* n $(n=0, 1, 2, \cdots)$ we mean

---

1) See P. Samuel, *Anneaux factoriels*, Publicações da Sociedade de Matemática de São Paulo, 1963, pp. 58-63.

2) A *ring* in this note always means a commutative ring with 1.

$$(x)^e = \prod_{x \in X} x^{e(x)}\,; \quad e(x): \textit{integer} \geqslant 0\,, \quad \sum_{x \in X} e(x) = n\,.$$

Let $M(X)$ be the set of all X-monomials. We note that card. $M(X)=$ card. $X=\aleph^*$, if $\aleph^*$ is not less than $\aleph_0$ (the cardinality of a countable set). For each element $(a_e)\in R^{M(X)}$, we consider the formal sum

$$(1) \qquad f = \sum a_e(x)^e\,; \quad a_e \in R\,, \quad (x)^e \in M(X)\,.$$

Let $\aleph$ be a cardinal number $\geqslant \aleph_0$. We call (1) an $\aleph$-*series with respect to X over R*, if card. $\{(x)^e \mid a_e \neq 0\} \leqslant \aleph$.

The set $R\{X\}_\aleph$ of all these $\aleph$-series forms a ring by the obvious operations. This we see readily even when $\aleph < \aleph^*$, taking account of the fact that then for any element f in $R\{X\}_\aleph$ there is a subset Y of X such that $f \in R\{Y\}_\aleph$ and card. $Y = \aleph$.

We denote by f_n $(n = 0, 1, 2, \cdots)$ the homogeneous part of degree n of an $\aleph$-series f. The subring $R\{X\}$ of $R\{X\}_\aleph$ consisting of those $\aleph$-series f such that f_n is a finite sum (a polynomial) for every n is nothing but the *usual formal power series ring*; that is, the (X)-adic completion of the polynomial ring $R[X]$, where (X) is the ideal of $R[X]$ generated by the set X. We note that although merely $R\{X\}_\aleph = R\{X\}$ if X is a finite set, otherwise necessarily $R\{X\}_\aleph \neq R\{X\}$.[3]

The above notations will be fixed throughout this note.

Lemma 1. *If R is an integral domain, then $R\{X\}_\aleph$ is an integral domain, and so is $R\{X\}$. An element $f \in R\{X\}_\aleph$ (or $\in R\{X\}$) is a unit if and only if the constant term of f is a unit in R.*

Proof. We may make X a well-ordered set. We order X-monomials by their degree, and then for X-monomials of the same degree we order lexicographically. Namely : $\prod x^{e(x)} < \prod x^{e'(x)}$, if either (i) $\sum e(x) < \sum e'(x)$ or (ii) $\sum e(x) = \sum e'(x)$ and $e(y) > e'(y)$ where y is the first variable such that $e(y) \neq e'(y)$. Thus we make $M(X)$ a well-ordered set in such a way that if m_1, m_2, m_3, and m_4 are four X-monomials with $m_1 \leqslant m_2$ and $m_3 \leqslant m_4$ then we have $m_1 \cdot m_3 \leqslant m_2 \cdot m_4$.

Let f and g be non-zero elements of $R\{X\}_\aleph$, and let $a_m \cdot m$

3) If $\aleph^* \geqslant \aleph_0$, the $\aleph$-series $\sum_{x \in Y} x$ of degree 1, where Y is a subset of X with card. $Y = \aleph_0$, is not in $R\{X\}$.

and $b_{m'}\cdot m'$ $(m, m'\in M(X);\ a_m, b_{m'}\in R)$ be the first monomials which appear with non-zero coefficients in f and g respectively. Then, clearly, $a_m\cdot b_{m'}\cdot m\cdot m'$ is the first monomial which actually occurs in $f\cdot g$. Thus $f\cdot g\neq 0$, and the first assertion is proved.

The second assertion is proved also by the same way as in the case of a finite number of variables; by virtue of the ordering of $M(X)$. q.e.d.

Lemma 2. *Let R be an integral domain and let Ω be the field of quotients of $R\{X\}$, then we have*

$$R\{X\} = R\{X\}_{\aleph}\cap\Omega\,.$$

Proof. Assume that there is an element f in $R\{X\}_{\aleph}\cap\Omega$ which is not contained in $R\{X\}$. Then f is an $\aleph$-series and we have

$$(2)\qquad f\cdot F = G\,,\quad \text{with}\quad F, G\in R\{X\}\,.$$

Let f_n, F_n, and G_n be the homogeneous parts of degree n of f, F, and G respectively. Let F_q be the leading form of F; that is, the homogeneous part $\neq 0$ of F of the least degree. Since $f\notin R\{X\}$, there exists an integer n for which f_n involves infinitely many variables actually. Of all these integers let n be the least. From (2),

$$(3)\qquad G_{n+q} = f_n\cdot F_q+\cdots+f_0\cdot F_{n+q}\,.$$

Both sides of (3), except for $f_n\cdot F_q$, involve only a finite number of variables. While $f_n\cdot F_q\neq 0$ and involves infinitely many variables actually among terms with non-zero coefficients, which is a contradiction. q.e.d.

2. We consider a well-ordering of X, and fix it henceforth. Let α be the ordinal number of the ordered set X. For each ordinal number $\xi<\alpha$, we denote by x_ξ the element y of X such that ξ is the ordinal number of $\{x\in X\mid x<y\}$; so that for each $\xi\leqslant\alpha$ the set $X_\xi=\{x_\nu\mid \nu<\xi\}$ has the ordinal number ξ.

For ξ and η with $\eta<\xi\leqslant\alpha$ and for any cardinal number $\aleph'$ not less than $\aleph$, we have the ring homomorphism, denoted by ρ^ξ_η,

$$(4)\qquad \rho^\xi_\eta:\ R\{X_\xi\}_{\aleph}\to R\{X_\eta\}_{\aleph'}\,;$$

by taking the residue class of each element of $R\{X_\xi\}_\aleph$ modulo the ideal generated by $\{x_\nu \mid \eta \leqslant \nu < \xi\}$. Then the following lemma follows readily from Lemma 1.

Lemma 3. *An element of* $R\{X_\xi\}_\aleph$ *is a unit if and only if its image by* ρ^ξ_η *is a unit.*

Lemma 4. *Assume that* $\aleph \geqslant \aleph^*$. *Let a transfinite sequence* $(f_\xi)_{\xi<\alpha}$ *be such that*:

$$(5) \qquad \begin{cases} f_\xi \in R\{X_\xi\}_\aleph , \\ \text{and} \quad \rho^\xi_\eta f_\xi \sim f_\eta \qquad \text{if } \eta < \xi.\text{[4]} \end{cases}$$

Then, there exists a $g \in R\{X\}_\aleph$ *such that* $\rho^\alpha_\xi g \sim f_\xi$ *for any* $\xi < \alpha$.

Proof. We shall define g_ν for every ν $(\leqslant \alpha)$, by transfinite induction, such that

$$(6) \qquad \begin{cases} g_\nu \in R\{X_\nu\}_\aleph , \\ g_\nu \sim f_\nu \quad \text{if} \quad \nu < \alpha , \\ \text{and} \quad \rho^\nu_\mu g_\nu = g_\mu \qquad \text{if } \mu < \nu \leqslant \alpha . \end{cases}$$

Set $g_1 = f_1$. Assume g_ν has been defined for every ν with $\nu < \xi$, so that (6) is satisfied.

Case 1. $\xi = \alpha$ and α is an isolated number.
Define $g_\xi = g_{\xi-1}$.

Case 2. ξ is an isolated number and $\xi < \alpha$.
As $\rho^\xi_{\xi-1} f_\xi \sim f_{\xi-1} \sim g_{\xi-1}$, we have $\rho^\xi_{\xi-1}(h_\xi \cdot f_\xi) = g_{\xi-1}$; where h_ξ is a unit in $R\{X_\xi\}_\aleph$ (Lemma 3). Define $g_\xi = h_\xi \cdot f_\xi$.

Case 3. $\xi = \alpha$ and α is a limit number.
For any given X_ξ-monomial $(x)^e$, there exists a $\nu (< \xi)$ such that $(x)^e$ is already a X_ν-monomial, and the coefficient of $(x)^e$ in g_ν is independent of the choice of ν. Therefore we can consider $\lim_{\nu<\xi} g_\nu \in R\{X_\xi\}_\aleph$. Define $g_\xi = \lim_{\nu<\xi} g_\nu$.

Case 4. ξ is a limit number and $\xi < \alpha$.
As $\rho^\xi_\nu f_\xi \sim f_\nu \sim g_\nu$ for any $\nu < \xi$, we have $\rho^\xi_\nu (h_\nu \cdot f_\xi) = g_\nu$; where h_ν is

4) $f \sim g$ means f and g are associates with each other.

a unit in $R\{X_\nu\}_\aleph$. As it is easily seen that $\rho^\nu_\mu h_\nu = h_\mu$, we can consider $\lim_{\nu<\xi} h_\nu = h_\xi \in R\{X_\xi\}_\aleph$. By Lemma 3, h_ξ is a unit in $R\{X_\xi\}_\aleph$. Define $g_\xi = h_\xi \cdot f_\xi$. q.e.d.

Theorem 1.[5] *If a ring R satisfies the condition $(*)$, then $R\{X\}_\aleph$ is a unique factorization domain.*

Proof. We use transfinite induction on $\aleph^*$ (= the cardinality of X). When X is a finite set, the assertion is trivial. Let $\aleph^* \geqslant \aleph_0$. Assume the assertion holds for variables of less cardinality.

Let α be the least ordinal number which has cardinality $\aleph^*$. We reorder X so that the ordinal type of the ordered set X is α. With respect to this ordering, let x_ξ, X_ξ, and ρ^ξ_η be as above. Then, for every $\xi < \alpha$, the cardinality of $X_\xi = \{x_\nu \mid \nu < \xi\}$ is less than $\aleph^*$; so that $R\{X_\xi\}_\aleph$ is a unique factorization domain by the induction assumption. We note that α is a limit number; for otherwise α is an isolated number (not finite), and therefore $\alpha - 1$ would also have cardinality $\aleph^*$.

Furthermore, we may assume $\aleph \geqslant \aleph^*$. Indeed, if $\aleph < \aleph^*$, then, letting Y run over all subsets of X such that card. $Y = \aleph$, we have $R\{X\}_\aleph = \cup R\{Y\}_\aleph$. The assertion in the case where $\aleph < \aleph^*$ follows from the facts that $R\{Y\}_\aleph$ is a unique factorization domain, that any finite number of elements of $R\{X\}_\aleph$ can be contained in a suitable $R\{Y\}_\aleph$ at the same time, and that an element of $R\{X\}_\aleph$ is irreducible if and only if it is so in a $R\{Y\}_\aleph$.

First we shall show that:

UF 1. *every element $f \neq 0$ of $R\{X\}_\aleph$ is expressed as a product of a finite number of irreducible elements.*

Write $\rho^\alpha_\nu f = f_\nu$. We consider a sufficiently large ν ($< \alpha$) such that $f_\nu \neq 0$. In the unique factorization domain $R\{X_\nu\}_\aleph$, let the factorization of f_ν into ireducible factors be

$$(7) \qquad f_\nu = h_\nu \cdot \prod_{i=1}^{m(\nu)} p_{\nu,i}{}^{e(\nu,i)};$$

5) The case where $\aleph \geqslant \aleph^*$ has been obtained by E. D. Cashwell and C. J. Everett, *Formal power series*, Pacific J. Math. **13**, 1963, pp. 45–64; D. Deckard, M. A. Thesis, Rice University, 1961; D. Deckard and L. K. Durst, *Unique factorization*, Pacific J. Math. **16**, 1966 pp. 239–242.

where h_ν is a unit, $p_{\nu,i}$ is an irreducible non-unit in $R\{X_\nu\}_\aleph$ such that $p_{\nu,i} \not\sim p_{\nu,j}$ for $i \neq j$. The number of non-unit factors in (7) is denoted by $d(\nu)$: $d(\nu) = \sum_{i=1}^{m(\nu)} e(\nu, i)$. If $\nu < \mu < \alpha$, then $f_\mu \neq 0$, and we get another factorization of f_ν by going down from μ:

$$(8) \qquad f_\nu = \rho_\nu^\mu f_\mu = (\rho_\nu^\mu h_\mu) \cdot \prod_{i=1}^{m(\mu)} (\rho_\nu^\mu p_{\mu,i})^{e(\mu,i)} .$$

In (8) we see that each foctor $\rho_\nu^\mu p_{\mu,i}$ $(1 \leqslant i \leqslant m(\mu))$ is a non-unit and $\rho_\nu^\mu h_\mu$ is a unit in $R\{X_\nu\}_\aleph$, by Lemma 3.

Since of all factorization of f_ν the factorization into irreducible factors has the largest number of non-unit factors, it follows from (7) and (8) that $d(\nu)$ is monotone decreasing with ν. Hence, there exists a ν_1 such that if $\nu_1 < \nu$, $d(\nu)$ is a constant: $= d$. When $d(\nu) = d$, each factor $\rho_\nu^\mu p_{\mu,i}$ in (8) $(\nu < \mu < \alpha, 1 \leqslant i \leqslant m(\mu))$ must be irreducible in $R\{X_\nu\}_\aleph$.

Consider μ and ν such that $\nu_1 < \nu < \mu$. Comparing once more (7) with (8), we see that $m(\nu) \leqslant m(\mu)$; since $m(\nu)$ is the number of distinct irreducible components of f_ν. This implies that $m(\nu)$ is monotone increasing with ν if $\nu_1 < \nu$. Moreover, $m(\nu)$ is upperly bounded since $\sum_{i=1}^{m(\nu)} e(\nu, i) = d$. Hence, there exists a ν_0 such that if $\nu_0 < \nu$, $m(\nu)$ is a constant: $= m$; and therefore if $\nu_0 < \nu$ $e(\nu, i)$ $(1 \leqslant i \leqslant m)$ must also be a constant: $= e_i$. Thus we get if $\nu_0 < \nu$,

$$(9) \quad \begin{cases} f_\nu = h_\nu \cdot \prod_{i=1}^{m} p_{\nu,i}{}^{e_i} & \textit{(factorization into irreducible factors in } R\{X_\nu\}_\aleph) \\ \rho_\nu^\mu p_{\mu,i} \sim p_{\nu,i} & (\nu_0 < \nu < \mu < \alpha\,,\ 1 \leqslant i \leqslant m) . \end{cases}$$

By using Lemma 4, we can find $q_i \in R\{X\}_\aleph$ $(1 \leqslant i \leqslant m)$ such that $\rho_\nu^\alpha q_i \sim p_{\nu,i}$ $(\nu_0 < \nu < \alpha, 1 \leqslant i \leqslant m)$. Let h'_ν be the unit in $R\{X_\nu\}_\aleph$ such that $f_\nu = h'_\nu \cdot \rho_\nu^\alpha (\prod_1^m q_i{}^{e_i})$. As $\rho_\nu^\mu h'_\mu = h'_\nu$ and α is a limit number, we can consider $\lim\limits_{\nu_0 < \nu < \alpha} h'_\nu = h' \in R\{X\}_\aleph$; where h' is a unit, by Lemma 3.

Thus we get a factorization of f in $R\{X\}_\aleph$:

$$(10) \qquad f = h' \cdot \prod_{i=1}^{m} q_i{}^{e_i} .$$

It is clear that every q_i is a non-unit, by Lemma 3. That every q_i is moreover irreducible follows from the fact that if q_i were factorized into two non-units, then, by going down to ν, $(q_i)_\nu \sim p_{\nu, i}$ would be factorized into two non-units. This completes the proof of UF 1.

Remark. The following is also a consequence of our argument above.

If f is irreducible, then f_ν is irreducible for sufficiently large $\nu(<\alpha)$.

(The converse is also true as we have seen above.)
Indeed, assume the contrary, suppose that f is irreducible and that there are ν arbitrarily large such that f_ν is reducible. Then we can find ν such that f_ν is reducible and ν is larger than ν_0 defined in (9). Therefore, in (9), $\sum_1^m e_i$ must be >1. Thus, we have $f=h'\cdot \prod_1^m q_i^{e_i}$, $\sum_1^m e_i>1$; by (10). As each q_i $(1\leqslant i\leqslant m)$ has been a non-unit, we obtain a contradiction.

Finally, we shall show that:

UF 2. *if $p|f\cdot g$ with $p, f, g\in R\{X\}_{\aleph}$ and if p is irreducible, then either $p|f$ or $p|g$.*

Indeed, let $\nu(<\alpha)$ be sufficiently large so that $(f\cdot g)_\nu \neq 0$, and that p_ν is irreducible (by Remark above). From $p|f\cdot g$ we have either $p_\nu|f_\nu$ or $p_\nu|g_\nu$. Therefore, we see that either the upper limit of the set $\{\nu|\nu<\alpha,\ f_\nu$ is divisible by $p_\nu\}$ or that of the set $\{\nu|\nu<\alpha,\ g_\nu$ is divisible by $p_\nu\}$ is equal to α. For otherwise, since α is a limit number, there would be a ν sufficiently large such that neither f_ν nor g_ν is divisible by p_ν.

We consider the case where the upper limit of the former is α. Then f_ν must be divisible by p_ν also for every $\nu(<\alpha)$; since if $\nu<\mu$ and $p_\mu|f_\mu$, then $p_\nu|f_\nu$. Write $f_\nu=p_\nu\cdot f'_\nu$, then $(f'_\nu)_{\nu<\alpha}$ satisfies the condition $\rho^\mu_\nu f'_\mu=f'_\nu$; and therefore we can consider $\lim_{\nu<\alpha} f'_\nu=f'$ in $R\{X\}_\aleph$. Thus we conclude $f=p\cdot f'$. This completes the proof of UF 2, and therefore of the theorem.

3. We remark that the question whether $R\{X\}_{\aleph}$ in Theorem 1 is replaced by $R\{X\}$, namely every q_i in (10) can be chosen as an usual formal power series when f is so, remains unsolved.

Now we shall consider $R\{X\}$ under a mild condition that R is a Krull ring. We recall[6] that an integral domain R is a Krull ring if and only if the following three conditions are satisfied:

KR 1. $R_{\mathfrak{p}}$ is a discrete valuation ring for any prime ideal $\mathfrak{p}$ of R of height 1.

KR 2a. Every principal ideal of R has only a finite number of prime divisors $\mathfrak{p}$ such that height $\mathfrak{p}=1$.

KR 2b. Letting $\mathfrak{p}$ run over prime ideals of height 1 in R, we have $R=\bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$.

Theorem 2. *If R is a Krull ring, then so is $R\{X\}$.*

Proof. Let K and Ω be the fields of quotients of R and $R\{X\}$ respectively. Let $\aleph$ be any cardinal number $\geqslant \aleph_0$. Let $\mathfrak{p}$ be a prime ideal of R of height 1. Since $R_{\mathfrak{p}}$ is a discrete valuation ring (KR 1.); using Theorem 1, we see that $R_{\mathfrak{p}}\{X\}_{\aleph}$ is a unique factorization domain, and therefore a Krull ring. Similarly, we see that $K\{X\}_{\aleph}$ is a Krull ring. Since, by Lemma 2, $K\{X\}$ is expressed as an intersection of $K\{X\}_{\aleph}$ and a field; $K\{X\}$ is also a Krull ring.[7]

Now, let V be the set consisting of those discrete valuation rings v of the field Ω, such that v is either equal to one of $v_{\mathfrak{q}}$ or equal to one of $v_{\mathfrak{q}_1}$ of the following types:

(i) $v_{\mathfrak{q}}=K\{X\}_{\mathfrak{q}}\cap\Omega$,
where $\mathfrak{q}$ *is a prime ideal of* $K\{X\}$ *of* height 1.

(ii) $v_{\mathfrak{q}_1}=[R_{\mathfrak{p}}\{X\}_{\aleph}]_{\mathfrak{q}_1}\cap\Omega$,
where $\mathfrak{p}$ *is a prime ideal of R of height* 1, *and* $\mathfrak{q}_1$ *is a prime ideal of* $R_{\mathfrak{p}}\{X\}_{\aleph}$ *of height* 1 *such that* $\mathfrak{q}_1$ *contains an element whose leading form has all coefficients in* $\mathfrak{p}R_{\mathfrak{p}}$.

---

6) As for the theory of Krull rings see, e.g., M. Nagata, *Local rings*, John Wiley, New York, 1962, pp. 115–118.

7) See Theorem (33. 6) and (33. 7), pp. 116–117, *idid.*

Owing to the criterion for a Krull ring,[8] we have only to prove that

1) if an element f of $R\{X\}$ is not zero, then there are only a finite number of v in V such that f is a non-unit in v;

2) $R\{X\}=\bigcap_{v\in V} v$.

Proof of 1). By virtue of KR 2a for $K\{X\}$, almost all prime ideals $\mathfrak{q}$ of height 1 in $K\{X\}$ do not contain the given f. ("almost all" means all but a finite number.) Whence we see that there are only a finite number of $v_{\mathfrak{q}}$ of type (i) in which f is a non-unit.

By virtue of KR 2a for R, there are only a finite number of common prime divisors $\mathfrak{p}$ of height 1 for all the coefficients of the leading form of the given f, For such a common prime divisor $\mathfrak{p}$, almost all prime ideals $\mathfrak{q}_1$ of height 1 in $R_{\mathfrak{p}}\{X\}_{\aleph}$ do not contain f; by KR 2a for $R_{\mathfrak{p}}\{X\}_{\aleph}$. While for a remaining prime ideal $\mathfrak{p}$ of R of height 1, in $R_{\mathfrak{p}}\{X\}_{\aleph}$ no prime ideal $\mathfrak{q}_1$ of height 1 contains both f and an element whose leading form has all coefficients in $\mathfrak{p}R_{\mathfrak{p}}$. (Note that a prime ideal of $R_{\mathfrak{p}}\{X\}_{\aleph}$ of height 1 is principal.) Thus we see that there are only a finite number of $v_{\mathfrak{q}_1}$ of type (ii) in which f is a non-unit.

Proof of 2). Clearly, $R\{X\}\subseteq\bigcap_{v\in V} v$. Conversely, let $f\in\bigcap_{v\in V} v$. Since $\bigcap_{\mathfrak{q}} v_{\mathfrak{q}}=K\{X\}$ by KR 2b for $K\{X\}$, we have

$$\bigcap_{v\in V} v=(\bigcap_{\mathfrak{q}} v_{\mathfrak{q}})\cap(\bigcap_{\mathfrak{p},\mathfrak{q}_1} v_{\mathfrak{q}_1})\subseteq K\{X\}\cap(\bigcap_{\mathfrak{p},\mathfrak{q}_1}[R_{\mathfrak{p}}\{X\}_{\aleph}]_{\mathfrak{q}_1}).$$

As an element of $K\{X\}, f$ can be written

$$(11)\qquad f=\sum a_e(x)^e,\quad a_e\in K\qquad (\textit{formal power series}).$$

We fix $\mathfrak{p}$ for a while. Then as an element of the field of quotients of $R_{\mathfrak{p}}\{X\}_{\aleph}$, f is also written

$$(12)\qquad f=G/F;\quad F, G\in R_{\mathfrak{p}}\{X\}_{\aleph},\quad F\neq 0.$$

Since $R_{\mathfrak{p}}\{X\}_{\aleph}$ is a unique factorization domain, we may assume that $(F, G)=1$ in (12); so that F and G in (12) are uniquely

8) See Theorem (33, 6), p. 116, *ibid.*

determined by f except for unit factors. Let F_q be the leading form of F. Let p be the prime element of $R_{\mathfrak{p}}$. (We note that p is also a prime element of $R_{\mathfrak{p}}\{X\}_{\aleph}$.) Then, $p\nmid F_q$ in $R_{\mathfrak{p}}\{X\}_{\aleph}$. For otherwise a minimal prime divisor $\mathfrak{q}_1$ of F in $R_{\mathfrak{p}}\{X\}_{\aleph}$ would satisfy the condition in (ii) above; and $F\in\mathfrak{q}_1$, $G\notin\mathfrak{q}_1$, so that $[R_{\mathfrak{p}}\{X\}_{\aleph}]_{\mathfrak{q}_1}$ would not contain $f=G/F$.

We shall show that every coefficient a_e in (11) must be in $R_{\mathfrak{p}}$. Assume the contrary. Of all the homogeneous parts of series (11) one of whose coefficients is not in $R_{\mathfrak{p}}$, let f_n be of the least degree. As f is a formal power series and therefore f_n is a polynomial with coefficients in K, we can write

(13) $f_n=f'_n/p^k$; k : integer > 0, $f'_n\in R_{\mathfrak{p}}\{X\}$, $(f'_n, p)=1$ in $R_{\mathfrak{p}}\{X\}_{\aleph}$.

From $f\cdot F=G$, we get

$$G_{n+q} = f_n\cdot F_q+\cdots+f_0\cdot F_{n+q}\,,$$

and so it follows that $f_n\cdot F_q\in R_{\mathfrak{p}}\{X\}_{\aleph}$. Therefore, by (13), we have $p^k|f'_n\cdot F_q$ in $R_{\mathfrak{p}}\{X\}_{\aleph}$; which contradicts to the fact that $p\nmid f'_n$, $p\nmid F_q$, and p is irreducible in $R_{\mathfrak{p}}\{X\}_{\aleph}$.

Thus, we have shown that in (11) every $a_e\in R_{\mathfrak{p}}$, where $\mathfrak{p}$ may be an arbitrary prime ideal of height 1 in R. Since $\bigcap_{\mathfrak{p}} R_{\mathfrak{p}}=R$ by KR 2b for R, it follows from this that every coefficient a_e in (11) must be in R, therefore $f\in R\{X\}$ as desired. This completes the proof of 2) and of the theorem.